East Asian Math. J.
Vol. 37 (2021), No. 5, pp. 585–590
http://dx.doi.org/10.7858/eamj.2021.037

JACOBIAN VARIETIES OF HYPERELLIPTIC CURVES OVER FINITE FIELDS WITH THE FORMAL STRUCTURE OF THE MIXED TYPE

Gyoyong Sohn

Abstract. This paper consider the Jacobian variety of a hyperelliptic curve over a finite field with the formal structure of the mixed type. We present the Newton polygon of the characteristic polynomial of the Frobenius endomorphism of the Jacobian variety. It gives an useful tool for finding the local decomposition of the Jacobian variety into isotypic components.

1. Introduction

There are several invariants associated with abelian varieties such as the p-rank, the Newton polygon, and the Ekedahl-Oort type. These invariants give information about the Frobenius morphism and the number of points of the abelian variety defined over finite fields. The study of invariants on hyperelliptic curves over finite fields has been studied by numerous researchers (e.g., [2, 3] and [4]). Based on the Newton polygon of the characteristic polynomial of the Frobenius endomorphism of the Jacobian variety, Yui gaves a classification of the Jacobian variety of a hyperelliptic curve over a field with characteristic $p > 0$ in [5]. In this paper, we consider the Jacobian variety of a hyperelliptic curve over a finite field with the formal sturcture of the mixed type. The formal group of the Jacobian vareity is the connected component of the p-divisible gorup of the Jacobian vareity.

Let $\mathbb{F}_q$ be a finite field with $q = p^n$ elements for prime $p > 2$. Let C be a hyperelliptic curve of genus g defined over $\mathbb{F}_q$ and J_C denote its Jacobian variety. Let $M_r = \sharp C(\mathbb{F}_{q^r})$ be the number of points of C defined over $\mathbb{F}_{q^r}$, for $r \geq 1$. The *zeta function of* C is

$$Z(C/\mathbb{F}_q, t) = \exp\Big(\sum_{r=1}^{\infty} M_r t^r / r\Big).$$

Received July 15, 2021; Accepted September 27, 2021.
2010 *Mathematics Subject Classification.* 11C10, 11G10, 11G25.
Key words and phrases. Jacobian variety, Hyperelliptic Curve.

©2021 The Youngnam Mathematical Society
(pISSN 1226-6973, eISSN 2287-2833)

By the Weil conjectures for curves [6, 7], the zeta function $Z(C/\mathbb{F}_q, t)$ can be written as

$$Z(C/\mathbb{F}_q, t) = \frac{L(C/\mathbb{F}_q, t)}{(1-t)(1-qt)},$$

where $L(C/\mathbb{F}_q, t)$ is the L-polynomial of C. Let l be a prime number $l \neq q$. Let $\mathbb{Z}_l$ be the ring of l-adic ingeters, and $\mathbb{Q}_l$ its quotient field. Let $T_l(J_C)$ be the l-th Tate module of J_C, and $V_l(J_C) = T_l(J_C) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ be the corresponding vector space over $\mathbb{Q}_l$. Then $T_l(A)$ is a free $\mathbb{Z}_l$-module of rank $2g$. The characteristic polynomial of the Frobenious endomorphism π_{J_C} of J_C is defined as

$$P(J_C/\mathbb{F}_q, t) = \det(\pi_{J_C} - tI_d \mid V_l(J_C)).$$

Then $P(J_C/\mathbb{F}_q, t) = t^{2g} L(C/\mathbb{F}_q, t)$. Furthermore, $L(C/\mathbb{F}_q, t)$ is factored as

$$L(C/\mathbb{F}_q, t) = \prod_{i=1}^{g} (1 - \alpha_i t)(1 - \overline{\alpha}_i t),$$

where each α_i is a complex number of absolute value $\sqrt{q}$ and $\overline{\alpha}_i$ denotes the complex conjugate of α_i. Moreover, $P(J_C/\mathbb{F}_q, t)$ is a monic polynomial of degree $2g$ with rational integer coefficients of the form

(1)
$$P(J_C/\mathbb{F}_q, t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + q a_{g-1} t^{g-1} + \cdots + q^{g-1} a_1 t + q^g$$

for all $a_i \in \mathbb{Z}$, $1 \leq i \leq g$. For simplicity, we write $P(t)$ instead of $P(J_C/\mathbb{F}_q, t)$.

Remark 1. Let v_p be the p-adic valuation of $\mathbb{Q}_p$ and let ν_p denote the unique extension of the p-adic valuation v_p to the algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$, normalized so that $\nu_p(p) = 1$. The Newton polygon of $P(t) = \sum_{i=0}^{2g} a_i t^i \in \mathbb{Z}[t]$ over $\mathbb{Q}_p$ is the lower envelope of the set of the points $\{(i, v_p(a_i)) | 0 \leq i \leq 2g\}$ in $\mathbb{R} \times \mathbb{R}$.

2. Cartier-Manin matrix

In this section, we recall the definition of the Cartier-Manin matrix in the case of hyperelliptic curves. Let $K = \mathbb{F}_q(C)$ be a function field of C of one variable over $\mathbb{F}_q$ and let K^p denote the subfield of p-th powers. Let Ω_K be the space of all differential forms of degree 1 on K and let x be a separably generating transcendental element in $K \backslash K^p$. Then every differential $\omega \in \Omega_K$ can be written uniquely as

$$\omega = d\lambda + a^p x^{p-1} dx$$

with $\lambda, a \in K$, $a^p \in K^p$. The *(modified) Cartier operator* $\mathcal{C} : \Omega_K \to \Omega_K$ is defined as $\mathcal{C}(\omega) = a dx$.

Let $\omega = (\omega_1, \ldots, \omega_g)$ be a basis of Ω_K^0. Then there are $g \times g$ matrix $A = (a_{ij})$ with coefficients in $\mathbb{F}_q$ such that

$$\mathcal{C}(\omega) = A^{(1/p)} \omega,$$

where $A^{1/p}$ denotes $a_{ij}^{1/p}$. The matrix A is called the *Cartier-Manin matrix* of the hyperelliptic curve C.

In [1], Manin showed that this matrix is related to the characteristic polynomial of the Frobenius endomorphism π_{J_C} modulo p. Then, we have the following theorem.

Theorem 2.1. *Let C be a curve of genus g defined over a finite field $\mathbb{F}_{p^n}$. Let A be the Cartier-Manin matrix of C and let $A_\pi = A \cdot A^p \cdot A^{p^2} \cdots A^{p^{n-1}}$. Let $\kappa(t)$ be the characteristic polynomial of the matrix A_π and $\chi(t)$ the characteristic polynomial of the Frobenius endomorphism of J_C. Then, we have*

$$\chi(t) \equiv (-1)^g t^g \kappa(t) \ (mod\ p).$$

Proof. See [1]. □

Note that this theorem provides a very efficient method to compute the characteristic polynomial of the Frobenius endomorphism and the group order of the Jacobian of C modulo p.

3. Jacobian variety of C

In this section, we present the Newton polygon of the characteristic polynomial of the Frobenius endomorphism of J_C with formal structure of the mixed type.

In [5], Yui gave a complete characterization of the ordinary Jacobian variety J_C of C whose Cartier-Manin matrix has determinant zero in $\mathbb{F}_q$. In the case of determinant $|A| = 0$, there are useful results to determines the algebraic structure of Jacobian variety J_C of C. Now we discuss the Jacobian variety J_C of C whose A has determinat zero in $\mathbb{F}_q$.

Theorem 3.1. *Suppose that the Cartier-Manin matrix A of C has the determinant $|A| = 0$ in $\mathbb{F}_q$ and the matrix $A_\pi = AA^{(p)} \cdots A^{(p^{n-1})}$ has rank 0. Then the characteristic polynomial $P(t)$ has the p-adic decomposition $P(t) = \prod_{i=1}^{2g}(t-\alpha_i)$ with $0 < \nu_p(\alpha_i) < n$.*

Theroem 3.1 gives a decomposition of $P(t)$ over $\mathbb{Q}_p$. Then we can factor $P(t)$ into the form

(2)

$$P(t) = \prod_{\substack{i=1 \\ \nu_p(\alpha_i)=n/2}}^{2s} (t-\alpha_i) \prod_{\substack{i=1, \\ \nu_p(\alpha_i)=0}}^{r} (t-\alpha_i)(t-\overline{\alpha}_i) \prod_{\substack{i=1, \\ 0<\nu_p(\alpha_i)<n/2}}^{g-s-r} (t-\alpha_i)(t-\overline{\alpha}_i),$$

where $2s$ (resp. r) the number of the p-adic roots α_i of $P(t)$ with $v_p(\alpha_i) = n/2$ (resp. 0) and $\overline{\alpha}_i = p^n/\alpha_i$. There are the algebraic structure of Jacobian variety J_C up to isogeny, in the cases $[s = g, r = 0]$, $[s = 0, r = 0]$, and $[0 < s < g, 0 < r < g]$, respectively. Now, we consider the Jacobian variety with the characteristic polynomial in the case $[s = 0, r = l]$ for some integer l.

Theorem 3.2. [5] *Suppose that the Cartier-Manin matrix A of C has the determinant $|A| = 0$ in $\mathbb{F}_q$ and the matrix $A_\pi = AA^{(p)} \cdots A^{(p^{n-1})}$ has rank 0. The following statements are equivalent :*
(a) $P(t) = \prod_{i=1}^{g}(t-\alpha_i)(t-\overline{\alpha}_i)$ with α_i simple roots, and $\nu_p(\alpha_i) = n\lambda$, $0 < \lambda < \frac{1}{2}$ for every $1 \le i \le g$,
(b) $P(t) = \sum_{i=0}^{2g} a_i t^i$ is a distinguished polynomial over $\mathbb{Z}_p$ and the coefficients a_i satisfy the condition:

$$\min_{0 \le i \le 2g} \frac{v_p(a_i)}{in} = \frac{v_p(a_g)}{gn} = \lambda = \frac{\mu_\lambda}{\mu_\lambda + \omega_\lambda},$$

where μ_λ, ω_λ are positive integers such that $1 \le \mu_\lambda < \omega_\lambda$, $(\mu_\lambda, \omega_\lambda) = 1$, and $\mu_\lambda + \omega_\lambda = g$.

Proof. See [5]. □

Now we consider the characteristic polynomila $P(t)$ of J_C with degree $g - l$ for positive integers l with $1 \le l \le g - 3$.

Lemma 3.3. *Suppose that the Cartier-Manin matrix A of C has the determinant $|A| = 0$ in $\mathbb{F}_q$ and the matrix $A_\pi = AA^{(p)} \cdots A^{(p^{n-1})}$ has rank 0. For positive interger l with $0 \le l \le g - 3$, let $P(t) = \prod_{i=1}^{g-l}(t - \alpha_i)(t - \overline{\alpha}_i)$ with α_i complex numbers, and $\nu_p(\alpha_i) = n\lambda$, $0 < \lambda < \frac{1}{2}$ for $1 \le i \le g - l$. Let $P(t) = \sum_{i=0}^{2(g-l)} a_i t^i$ is a polynomial over $\mathbb{Z}_p$. Then we have the coefficients a_i satisfy the condition:*

$$v_p(a_{g-l}) = (g - l)n\lambda \text{ and } v_p(a_{(g-l-i)}) \ge (g - l - i)n\lambda$$

where μ_λ, ω_λ are positive integers such that $1 \le \mu_\lambda < \omega_\lambda$, $(\mu_\lambda, \omega_\lambda) = 1$, and $\mu_\lambda + \omega_\lambda = g - l$, and $\lambda = \frac{\mu_\lambda}{\nu_\lambda + \omega_\lambda}$.

Proof. Suppose that the characteristic polynomial $P(t)$ has the following form : $P(t) = \prod_{i=1}^{g-l}(t - \alpha_i)(t - \overline{\alpha}_i)$ with $\nu_p(\alpha_i) = \lambda n$, $0 < \lambda < \frac{1}{2}$ for $1 \le i \le g - l$. It is the case of $s = 0$ and $r = 0$ in (2). Put $\overline{\alpha}_i = \alpha_{g-l+i}$ for $1 \le i \le g - l$. Then we have $\nu_p(\alpha_i) = \lambda n$, $\nu_p(\alpha_{g-l+i}) = (1 - \lambda)n$ for $1 \le i \le g - l$, from which we have that $v_p(a_0) = 0$, $v_p(a_i) \ge \lambda in$ for every $1 \le i \le g - l$, $v_p(a_{g-l}) = \lambda(g - l)n$, and $v_p(a_{g-l+i}) \ge \lambda(g - l)n + (1 - \lambda)in$ for $1 \le i \le g - l$. Hence it follows that

$$\frac{v_p(a_i)}{in} \ge \lambda, \ \frac{v_p(a_{g-l})}{(g - l)n} = \lambda, \text{ and } \frac{v_p(a_{g-l+i})}{(g - l + i)n} \ge \lambda.$$

Therefore, we get

$$\min_{0 \le i \le 2(g-l)} \frac{v_p(a_i)}{in} = \frac{v_p(a_{g-l})}{(g - l)n} = \lambda.$$

Now put $\mu_\lambda = \lambda(g - l)$ and $\omega_\lambda = g - l - \mu_\lambda = (1 - \lambda)(g - l)$. Then μ_λ, ω_λ are positive integers satisfying $1 \le \mu_\lambda < \omega_\lambda$, $\mu_\lambda + \omega_\lambda = g - l$, $(\mu_\lambda, \omega_\lambda) = 1$, and $\lambda = \mu_\lambda/(\mu_\lambda + \omega_\lambda)$. □

Our main result is the following theorem.

Theorem 3.4. *Suppose that the Cartier-Manin matrix A of C has the determinant $|A| = 0$. The following statements are equivalent :*
(a) If the characteristic polynomial $P(t)$ of Jacobian vareity J_C is decomposed into the product $P_1(t)$ and $P_2(t)$, where $P_1(t) = \prod_{i=1}^{2l}(t-\alpha_i)$ with $\nu_p(\alpha_i) = n/2$ for positive integer l, $1 \leq l \leq g-3$ and $P_2(t) = \prod_{i=1}^{g-l}(t-\alpha_i)(t-\overline{\alpha}_i)$ with $\nu_p(\alpha_i) = \lambda n$ for $0 < \lambda < 1/2$.
(b) The arbitary polynomial over $\mathbb{Z}_p$ denote $P(t) = \sum_{i=0}^{2g} a_i t^i$ and the coefficients a_i satisfy the condition:

$$v_p(a_{(g-l)+i}) \geq \Big(\mu_\lambda + \frac{i}{2}\Big)n$$

for $1 \leq i \leq l$, and

$$v_p(a_{g-l}) = (g-l)n\lambda \text{ and } v_p(a_{g-l-j}) \geq (g-l-j)n\lambda$$

for $1 \leq j \leq g-l-1$ where λ, μ_λ, ω_λ are positive integers satisfying $1 \leq \mu_\lambda < \omega_\lambda$, $(\mu_\lambda, \omega_\lambda) = 1$, $\mu_\lambda + \omega_\lambda = g-l$ and $\lambda = \frac{\mu_\lambda}{\mu_\lambda+\omega_\lambda}$.

Proof. Assume (a). Then $P(t) = P_1(t)P_2(t)$ has the form

$$P(t) = \prod_{\substack{i=1 \\ \nu_p(\alpha_i)=n/2}}^{2l}(t-\alpha_i) \prod_{\substack{i=1, \\ 0<\nu_p(\alpha_i)<n/2}}^{g-l}(t-\alpha_i)(t-\overline{\alpha}_i), \tag{3}$$

for positive integer l, $1 \leq l < g-3$. Let $P_1(t) = \sum_{i=1}^{2l} b_i t^i$ be a polynomial over $\mathbb{Z}_p$. Then we have $v_p(b_i) = in/2$ for every $0 \leq i \leq 2l$.

Let $P_2(t) = \sum_{i=1}^{g-l} d_i t^i$ be a polynomial over $\mathbb{Z}_p$. Note that we can find positive integers λ, μ_λ, ω_λ such that $1 \leq \mu_\lambda < \omega_\lambda$, $(\mu_\lambda, \omega_\lambda) = 1$, $\mu_\lambda + \omega_\lambda = g-l$ and $\lambda = \frac{\mu_\lambda}{\mu_\lambda+\omega_\lambda}$. By Lemma 3.3, we have $v_p(d_{g-1}) = (g-l)n\lambda$ and $v_p(d_{g-l-i}) \geq (g-l-i)n\lambda$. Now the factorization $P(t) = P_1(t)P_2(t)$ gives $v_p(a_{g-l}) = \sum_{i=1,\nu_p(\alpha_i)=\lambda n}^{g-l} \nu_p(\alpha_i) = (g-l)n\lambda$, $v_p(a_{(g-l)+i}) \geq \lambda(g-l)n + in/2 = (\mu_\lambda + i/2)n$ for $1 \leq i \leq 2l$, and $v_p(a_{g-l-j}) \geq (g-l-j)n\lambda$ for $1 \leq j \leq g-l-1$. □

Theorem 3.5. *If the characteristic polynomial $P(t)$ of the Jacobian vareity J_C of C has the form (3), then the Newton polygon of $P(t)$ has the segments L_1, L_2, L_3 from the right with slopes $-\lambda n$, $-n/2$ and $-(1-\lambda)n$, respectively. The Newton polygon of $P(t)$ is represented in Figure 1.*

Proof. By the Theorem 3.4, the Newton polygon has the segments L_i, $1 \leq i \leq 3$ with line equations $y = -\lambda n x + 2g\lambda n$, $y = -\frac{n}{2}x + (\frac{g+l}{2} + \mu_\lambda)n$ and $y = -(1-\lambda)nx + ng$ respectively. □

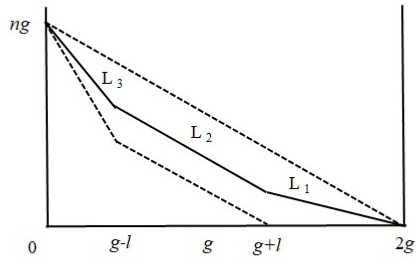

FIGURE 1.

References

[1] Yu. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, AMS Trans. Ser. 2, **45** (1965), 245–264.

[2] F. Oort, *Hyperelliptic supersingular curves*, Arithmetic algebraic geometry (Texel, 1989), Progr. math.,**89**, birkhäuser Boston, Boston, MA, (1991), 247–284.

[3] R. Pries, *The p-torsion of curves with large p-rank*, Int. J. Number Theory **5** (2009), no. 6, 1103–1116.

[4] J. Scholten and H. J. Zhu, *Hyperelliptic curves in characteristic 2*, Int. Math. Res. Not. (2002), no. 17, 905-917.

[5] N. Yui, *On the Jacobian Varieties of Hyperelliptic Curves over Fields of Characteristic* $p > 2$, Journal of Algebra **52** (1978), no. 2, 378–410.

[6] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041, Hermann et Cie.. Paris, 1948.

[7] A. Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064, Hermann & Cie., Paris, 1948.

GYOYONG SOHN
DEPARTMENT OF MATHEMATICS EDUCAITON, DAEGU NATIONAL UNIVERSITY OF EDUCATION, REPUBLIC OF KOREA
E-mail address: gysohn@dnue.ac.kr